PP Presentation

Routing Attacks

- Hit-and-Run Attack: hard to detect/isolate
  - Inject one (or very few) bad packet causing long term damage.
- Persistent Attack:
  - The intruder has to continuously inject attack packets.
- Attack Experiments:
  - Max-Sequence Number attack (implem. bugs).
  - MaxAgeDiff attack (weak checksum algo.)

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Sequence #: Counter Flushing

ATM

(1) Seq#: 0x7FFFFFFF

(2) 0x7FFFFFFF with

MaxAge to purge

this entry.

(3) 0x80000001.

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Attack and Fight-Back

ATM

Seq#

(1) 0x90001112

(2) 0x90001113

(3) 0x90001114

fight-back

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

MaxSeq# Attack

ATM

Seq#

(1) 0x90001112

(2) 0x7FFFFFFF

MaxSeq#

(3) 0x80000001

fight-back

(4). 0x7FFFFFFF

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

Max-Sequence Number Attack: Features

- Hit-and-Run attack (hard to identify/isolate)
- Implementation Bug! (confirmed in two independent and well known packages)
- Reason: MaxSeq# LSA Purging has not been implemented correctly!!
- Impact: The intruder can "control" the topology database for up to an hour.

Previous slide Next slide Back to the first slide View Graphic Version

Probabilistic MaxAgeDiff Attack

Probabilistic MaxAgeDiff Attack

- "Sort-of" Hit-and-Run Attack on the RFC directly.
- Preventable by OSPF Digital Signature.
- Still in progress (not yet implemented, and could be a fake attack). We need to verify the timing information in our OSPF routing testbed.

Previous slide Next slide Back to the first slide View Graphic Version

Undetected Tampering

Undetected Tampering

ATM

Seq#

(1) 0x90001112

- 0x90001112

the same checksum

but different value

They are the same, so not

take or forward .

Previous slide Next slide Back to the first slide View Graphic Version

Fresher LSA?

Fresher LSA?

Seq#A ? Seq#B

ChS:A ? ChS:B

AgeA-AgeB

=

=

>

>

<

<

A

A

A

B

B

B

15

-15

otherwise

A, B are treated the same.

Previous slide Next slide Back to the first slide View Graphic Version

Linear Case: LSA Age.

Linear Case: LSA Age.

E

D

C

B

15:0 14:0 16:0 15:0 0:0

15:1 14:1 16:1 0:1 0:1

15:2 14:2 0:2 0:2 0:2

15:3 14:3 0:3 0:3 0:3

Less than 15 minutes

STOP Here!

I don't

know...

A

Previous slide Next slide Back to the first slide View Graphic Version

Attacker's (E) Learning Phase

Attacker's (E) Learning Phase

1. Wait for MaxAgeDiff (15 minutes) before mess-up one LSA (the same Seq#, the same checksum, but 0 age.)
2. Check if the originator(A) fight-back or not:
   - If YES, try
     - MaxAgeDiff +delta
   - If NO, try
     - MaxAgeDiff - delta

Attacker

Victim

Previous slide Next slide Back to the first slide View Graphic Version

MaxAgeDiff Attack

MaxAgeDiff Attack

- Learning Phase:
  - Find out the optimal timing to control the largest possible area of good routers.
  - The learning itself can be undetectable.
- Attack Phase:
  - Launch one bad LSA after the optimal timing.
  - The network topology may be partially controlled for about 15 minutes.
    - LSRefreshInterval - MaxAgeDiff = 30 - 15 = 15.

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

What's Next:

- Implement the module code
- Collect more routing traffic statistical profiles
- Conduct code analysis on GateD (OSPF portion)
- Construct simulator to understand the impact of attack on a large scale network

Previous slide Back to the first slide View Graphic Version

MCNC electronic and information technologies

ADVANCED NETWORKING RESEARCH (ANR)

The Advanced Networking Research group at MCNC engages in a variety of research and development projects, involving security solutions for protection of information infrastructures and system solutions for high-speed networking. In addition to its independent R & D projects funded by federal agencies such as DARPA, the group also provides development and consulting services to other technology developers and users.

Projects Highlights

- **CELESTIAL**
  - Development of a security service management architecture for heterogeneous networking environment
  - Enhancing the survivability of networking infrastructures and promoting wide deployment of security services
- **Ji-Nao**
  - Development of an intrusion detection system for emerging internetwork environment
  - Provide protection for the routing infrastructure through SNMP-integrated solution
- **Enigma2**
  - Development of a cell-level security system for ATM/SONET public network standards
  - Provides full-bandwidth, full-duplex encryption at OC-12c (622Mbps) and OC-3c (155Mps)
- **Integrated QoS**
  - Porting/implementation of QoS provisioning protocols and mechanisms in NetStar GigaRouter
  - Evaluation through experiments and comparisons
- **Attila**
  - Development of a Dynamic BISDN Traffic Analysis System
  - Built around the ATM and SONET public network standards
- **VISTAnet**
  - Research in communications, graphics, and medical applications utilizing a gigabit testbed
  - One of the five gigabit network testbeds that have been selected for funding by the Corporation for National Research Initiatives as part of a program supported by NSF and ARPA
-

MCNC Homepage

MCNC
Post Office Box 12889
Research Triangle Park
North Carolina 27709-2889

June 1997

PP Presentation

New Ideas

Impact

Schedule

- Comprehensive approach for intrusion detection on network

infrastructure

- Offering prevention, detection, response, and reconfiguration capabilities

- Flexible architecture design which can target at any network

protocol of interest (select three key protocols: OSPF, PNNI, and SNMP as implementation examples)

- Coupling with network management to enable automated

responses and easy integration with other systems

- Providing comprehensive capabilities to protect network

infrastructures

- Resulting better understanding in security implications of

key network protocols

- Contributing to the IETF and vendors community regarding the

the finding of security vulnerabilities in protocol specification

and implementation

- Easy integration to be part of a fault management system

through the built-in network management component

- Can be commercialized/deployed to operational network

routers/switches

Start

JiNao IDS architecture

specification complete

Statistical profile

delivery

Modules code

delivery

Demo of JiNao

system implementation

Demo of JiNao

implementation

after refinement

Evaluation

Final

report

Scalable Intrusion Detection for the Emerging Network Infrastructure (JiNao)

Back to the first slide View Graphic Version

PP Presentation

ANR

MCNC

PP Presentation